UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

22-CR-109 (LJV)

v.

PAYTON GENDRON,

Defendant.

MOTION FOR AN ADJOURMENT OF THE TRIAL DATE AND FOR A FURTHER PRETRIAL SCHEDULING ORDER

Defendant, Payton Gendron, through undersigned counsel, hereby moves this Court for an adjournment of the current trial date, an extension of time to file motions to suppress evidence, and for a further pretrial scheduling order addressing areas of litigation in advance of trial that are not contemplated in the current scheduling order. This motion is based on the Fifth, Sixth and Eighth Amendments and the additional authorities cited herein.

Due to the issues created by the government's production of discovery and reproduction with new bates numbers in October 2024, and the need for additional time to file and litigate suppression motions, the additional pretrial litigation not covered by the current scheduling order, and the need for additional time for investigation, the defense requests an adjournment of the start date of the trial presently scheduled for September 8, 2025, to allow for jury selection to commence with potential jurors completing juror questionnaires the week of June 22, 2026, and the commencement of in-person voir dire on September 8, 2026. To the extent this filing is supported by privileged information about the progress of the defense team's trial preparation and strategy, including a recitation of tasks completed and those matters that remain ongoing, those portions are filed separately under seal and *ex parte* for the Court's consideration.

The requested adjournment is necessary to comport with the Sixth Amendment's requirement for effective assistance of counsel. It is also reasonable when compared to data from all other Second Circuit death penalty trial cases from 2005 to the present.[1] In that time, there have been 15 capital prosecutions that have gone to trial. The time from the initial federal charge in this case to the current September 2025 trial date is approximately 39 months. In contrast, the average time to trial for capital cases in the Second Circuit over the last twenty years is 53.4 months.

Defendant	Docket No.	Victim Count	Status	Charged	Auth Date	Trial Start	Charge to Trial (Months)	Auth to Trial (Months)
Williams, Elijah Bobby	SDNY 1:00-CR-1008	3	Life-jury	9/26/00	2/4/03	3/22/05	53.9	25.6
Williams, Michael	SDNY 1:00-CR-1008	3	Life-jury	9/26/00	2/4/03	3/22/05	53.9	25.6
Aguilar, Martin	EDNY 1:01-CR-1367	1	Life-jury	12/10/01	5/14/04	10/30/06	58.7	29.5
Caraballo, Gilberto	EDNY 1:01-CR-1367	2	Life-jury	12/10/01	5/14/04	1/14/08	73.1	44.0
James, Richard	EDNY 1:02-CR-778	2	Life-jury	6/27/02	8/1/03	3/26/07	57.0	43.8
Mallay, Ronald	EDNY 1:02-CR-778	2	Life-jury	9/27/02	8/1/03	3/26/07	54.0	43.8
Henderson, Darryl	SDNY 1:02-CR-451	3	Acquittal	4/16/02	2/23/05	11/8/06	54.7	20.5
Pepin-Taveras, Humberto	EDNY 1:04-CR-156	2	Life-jury	2/20/04	3/3/05	9/15/08	54.8	42.4
Barnes, Khalid	SDNY 1:04-CR-186	2	Life-jury	2/27/04	1/19/06	2/11/08	47.5	24.7
Wilson, Ronell	EDNY 1:04-CR-1016	2	Death Rev	3/12/03	8/2/05	10/11/06	43.0	14.3
McGriff, Kenneth	EDNY 1:04-CR-966	2	Life-jury	1/18/05	3/22/06	11/27/06	22.3	8.2
Basciano, Vincent	EDNY 1:05-CR-60	1	Life-jury	1/26/05	4/2/07	3/1/11	73.2	47.0
McTier, James	EDNY 1:05-CR-401	3	Life-jury	5/20/05	1/14/07	10/15/07	28.8	9.0
Aquart, Azibo	D.CT 3:06-CR-160	3	Death Rev	9/2/05	1/29/09	4/6/11	67.1	26.2
Saipov, Sayfullo Habibullaevic	SDNY 1:17-CR-722	8	Life-jury	11/1/17	9/28/18	10/11/22	59.3	48.4
							801.2	**453.2**
						Average:	**53.4**	**30.2**

As we demonstrate herein, though we have endeavored to be ready for the current trial date, we are not able to achieve that goal for several reasons. First, Payton Gendron's case is simply more complex than the other capital cases tried in this Circuit. The number of victims is significantly higher than any of the Second Circuit cases apart from *United States v. Saipov,* 17-CR-0722 (VSB) SDNY. Surviving family member witnesses are critically important at the penalty phase. In addition to the ten deceased victims, there are three injured victims who

[1] *See* Declaration of Matthew Rubenstein, Director of the Capital Resource Counsel (CRC) project, annexed hereto as Exhibit A.

survived and an additional 69 individuals in various locations both inside and outside the store that the government has charged as victims of the hate crimes and who it has alleged were placed at grave risk of death. This case has also generated an outsized amount of media coverage, spawned dual state and federal prosecutions, and further generated parallel civil proceedings – no less than four civil cases in total on behalf of 37 plaintiffs. To say this case is both complex and high profile is an understatement. For these reasons, this case requires more investigation and more careful consideration of penalty phase themes than the average capital case. Further, the amount of digital discovery and its critical importance in this case dwarfs that in the comparison cases. In this case, the government provided more than 4 *terabytes* of digital discovery. This evidence is important for the guilt and penalty phases as it provides insight into Payton Gendron's intent and the government's case in aggravation.

In addition to the time necessary to complete investigations, there remains significant litigation to be addressed in advance of trial.

I. Procedural History

a. From Indictment to the Notice of Intent to Seek the Death Penalty

On July 14, 2022, the grand jury charged Payton Gendron with capital eligible offenses in a 27-count indictment related to the killings of 10 people and the wounding of three others at the Tops grocery store in Buffalo on May 14, 2022. ECF No. 6. He is charged under 18 U.S.C. § 249(a)(1)(B)(3), the federal hate-crime statute, and 18 U.S.C. § 924(j), the federal firearms statute.

Following his arraignment on the Indictment, at a status conference on March 10, 2023, Magistrate Judge Schroeder granted defendant's motion to designate this case as complex pursuant to Title 18 U.S.C. § 3161(h)(7)(B)(ii), finding that due to the large volume of discovery

provided in this case, as well as the potential for a death penalty prosecution, counsel's obligations and professional responsibilities justify the designation. ECF No. 74 at 3-4. The government did not oppose this request. ECF No. 74 at 8.

Defense counsel were immediately focused on preparing their mitigation case to be submitted to the local United States Attorney's Office. In fact, the government began pressing for that meeting to occur in correspondence on June 16, 2022, before an indictment was even returned. The government initially scheduled the local mitigation meeting to take place on July 18, 2022. When defense counsel responded that a formal mitigation meeting so soon would be extremely premature, the government proposed that the meeting take place on August 1, 2022, and later on November 15, 2022. Counsel notified the government of the team's unavailability on November 15th and urged that, given the volume of discovery produced on September 21, 2022, significantly more time was needed to continue our investigation in accordance with our ethical obligations, including review of the discovery material. Defense counsel requested a date in March 2023. The government declined that request and re-scheduled the meeting to December 2, 2022. When an outbreak of COVID infected defense team members, that meeting was adjourned. Over defense counsel's continued insistence that this time frame was insufficient, the government rescheduled the meeting for January 5, 2023. On that date the defense team appeared at the local United States Attorney's Office to attempt to persuade the government not to seek the death penalty.

Countless hours were expended preparing a written submission in advance of this local presentation. A written submission was provided to the government on January 4, 2023. Additional events, prompted a supplemental submission in March 2023.

Thereafter, defense counsel were advised that a meeting would be scheduled to present the mitigation case to the Department of Justice, Capital Case Review Committee ("CCRC"). Again, defense counsel's requests to postpone that meeting until a full and complete investigation could be completed were likewise wholly rejected. The government scheduled the meeting with the CCRC for September 18, 2023. In preparation for that meeting, counsel prepared both a written submission and a Power Point presentation to convey their case, at that stage of the mitigation investigation, against seeking the death penalty. Following that meeting, the defense team prepared additional submissions, which were provided to the government on September 21, 2023, and October 6, 2023.

On January 12, 2024, roughly four months after defense counsel's presentation to the CCRC and eighteen months from the filing of the Indictment, the government filed its Notice of Intent to Seek the Death Penalty ("NOI") on Counts 11-20 of the Indictment. ECF No. 125. This would later prove to be the only case in which seeking the death penalty was authorized under the Biden Administration. The Notice alleged four statutory aggravating circumstances, and further alleged other non-statutory aggravators, including victim impact, injury to surviving victims, racially-motivated killings, attempt to incite violence, and selection of site. *Id*.

b. The Setting of the Current Scheduling Order and the Litigation to Date

Following the filing of the NOI, this Court held a status conference on February 2, 2024, to address the setting of a pretrial scheduling order for litigation. Over the defense objection, the Court set an aspirational trial date, seventeen months hence, for September 8, 2025. In addition to setting a trial date, the Court set a scheduling order for the filing of certain, but not all, pretrial motions. With one notable exception (suppression motions discussed more fully herein), the

parties have largely held to the scheduling order with brief extensions. Much litigation has ensued in the interim fourteen months.

At the status conference on February 2, 2024, the Court heard argument on Defendant's Motion for a Protective Order to Prohibit Prosecution Access to Defendant's Pretrial Detention Records (ECF No. 15) which had been filed on July 28, 2022, and supplemented on August 18, 2023, to reflect the change in Payton Gendron's custodial placement (ECF No. 99).[2] The Court allowed the parties to submit additional briefs (*see* ECF No. 135), which were filed on February 23, 2024, (ECF No. 140); March 15, 2024 (ECF No. 144); and March 22, 2024 (ECF No. 146). By Decision and Order entered April 29, 2024, the Court ruled, *inter alia*, that Payton Gendron presented good cause for a protective order that allows his counsel to review the pretrial detention records before those records are turned over to the government. *See* ECF No. 156. On May 31, 2024, the Court issued Orders to both the Erie County Holding Center (ECHC) and the Livingston County Jail (LCJ) directing the facilities to provide responsive records no later than June 21, 2024.

To facilitate the remaining steps outlined by the Court's Order (ECF No. 156), the parties jointly agreed to a procedure, which was submitted to the Court on July 25, 2024 (ECF No. 194-1) and subsequently adopted. ECF No. 195. Defense counsel produced their log on August 2, 2024 (ECF No. 202), and the government responded on August 16, 2024 (ECF No. 200 at 7).

On August 20, 2024, the Court denied without prejudice the request for additional information (ECF No. 206) and on August 30, 2024, the government filed its motion for disclosure of all pretrial detention records not protected by a constitutional claim or legal

[2] The government opposed the motion, ECF No. 92, but agreed not to pursue obtaining Payton Gendron's pretrial detention records while the motion was pending.

privilege. ECF No. 208 at 3. Additional pleadings were filed by the defense on September 27, 2024, (ECF No. 220) and by the government on October 18, 2024 (ECF No. 227). The Court ordered defense counsel to provide unredacted copies of all redacted and withheld records for the Court's *in camera* review (ECF No. 250), and the defense complied on December 9, 2024. ECF No. 265. By Decision and Order entered January 24, 2025, the Court granted the government's motion in part and denied it in part, ordering defense counsel to produce the records as described to the government by February 3, 2025, as extended. After seeking further clarification from the Court, counsel produced the records accordingly.[3]

At the status conference on February 2, 2024, the Court also set a calendar for pleadings related to the Fed.R.Crim.P. 12.2 litigation schedule. Defense counsel were directed to file their Memorandum in Support of their Proposed Schedule for 12.2 litigation by February 16, 2024. The Government's Response in Opposition was filed on February 23, 2024, and Defendant's Reply was filed on March 1, 2024. In compliance with the Court's Text Order, the government's motion to establish procedures for Rule 12.2 proceedings was filed on February 3, 2025, and defendant's response on March 3, 2025.

Also pursuant to the scheduling order established on February 2, 2024, the defense filed a Motion for an Informational Outline (ECF No. 160) and a Motion for a Bill of Particulars (ECF No. 161) on May 2, 2025. Thereafter, the Government provided a Bill of Particulars on

[3] The Court also ordered the facilities to produce records on a rolling basis and ordered defense counsel, within 14 days of receipt of new records, to disclose the records to the government, with records withheld or redacted in the same manner as ordered by the Court. The Court further ordered that Gendron must provide a disclosure log with each production to identify the records that LCJ produced, any redacted or withheld records, and the reasons for nondisclosure. No further records have been produced by LCJ since the original production.

September 10, 2024 (ECF No. 209) and an Informational Outline on September 13, 2024. (ECF No. 210).

On June 10, 2024, the defense team filed several constitutional motions, including the following:

- Motion to Dismiss Indictment Based on Unconstitutionality of Federal Hate Crimes Act, 18 U.S.C. §249(a)(1) (ECF No. 179);[4]
- Motion to Dismiss Counts 11-20 of Indictment for Failure to State an Offense Under 18 U.S.C. § 924(c) (ECF No. 180);
- Motion to Strike the Death Penalty as a Possible Punishment in this Case (ECF No. 181); and
- Motion to Categorically Exempt Payton Gendron from the Death Penalty Because He was Eighteen Years Old at the Time of the Alleged Capital Crimes (ECF No. 182).

As to the latter two constitutional motions, the Court issued a Text Order granting the defense request for a hearing to afford Payton Gendron the opportunity to present proof that his execution for crimes committed during late adolescence would violate the Eighth Amendment (the *Roper* extension issue). The Court further granted defense counsel's request to supplement its arbitrariness claim under its challenge to the FDPA, and directed the defense to provide written proffers of evidence for the Court to consider in support of its contentions that the federal death penalty is unreliable due to the death qualification of jurors; is unreliable due to the high rate of trial errors in capital cases; is arbitrary and cruel due to excessive delays; and is increasingly disfavored. *See* ECF No. 273 at 17-19. The Court set deadlines in February through May for the submissions related to these two motions. In accordance with those deadlines, on March 3 and 4, 2025, the defense provided its Rule 16 expert disclosures for the witnesses it intends to call at a *Roper* extension hearing, and on March 10, 2025, filed its supplement to the

[4] In a Decision and Order issued on March 12, 2025, the Court denied this Motion to Dismiss.

arbitrariness claim on the FDPA and related discovery demands. The government filed its expert disclosures for the *Roper* hearing on March 17, 2025, noting its intention to call five expert witnesses. This hearing, which will require extensive preparation, is expected to be held in May 2025.

As relevant to the Motion to Dismiss Counts 11-20 of Indictment for Failure to State an Offense Under 18 U.S.C. § 924(c) (ECF No. 180), following initial oral argument on November 15, 2024, the Court heard additional argument on February 7, 2025, and requested supplemental briefing to be submitted by the defense on February 28, 2025. The government filed its response on March 21, 2025; the defense reply is now due on April 7, 2025, in conjunction with a supplemental submission addressing the effect of the Supreme Court's decision in *Delligatti v. United States*, 604 U.S. ___ (2025) on this claim. *See* ECF No. 299. The government's supplemental submission is due April 21, 2025, and the defense reply by April 28, 2025.

On November 4, 2024, defense counsel filed a Motion to Dismiss Count 27 (ECF No. 234) as well as a Motion to Dismiss the Notice of Intent to Seek the Death Penalty for Abuse of the Grand Jury (ECF No. 235). The latter was taken on submission while oral argument on the former was held on March 12, 2025. At oral argument, the Court ordered further briefing to address *United States v. Rui Jiang*, No. 24-cr-65-RDA, ECF No. 96 (E.D. Va. Feb. 6, 2025), which was filed by the defense on March 19, 2025, and replied to by the government on March 25, 2025.

On November 29, 2024, defense counsel filed its Motion to Suspend the Scheduling Order and to Compel Discovery Production in a Usable Format. That motion alerted the Court to ongoing discovery issues related to the government's failure to identify relevant attachments to law enforcement reports, an issue the defense had been attempting to resolve with the

government since July 2024. These issues were exacerbated by the government's reproduction of a large volume of discovery with an entirely new set of Bates numbers untethered to the initial numbering. At a status conference on December 11, 2024, the Court ordered the government to "identify by original Bates number all attachments associated with each report and to provide the original Bates number for all documents it reproduced with a new Bates number" by January 13, 2025. (ECF No. 253.) Following two extensions of time to comply with the Court's Order, (ECF Nos. 259, 263), and the rescheduling of a status conference to address its compliance, the government produced a revised copy of its manifest in purported compliance with the Court's December 11, 2024, Text Order the night before a status conference scheduled to address these issues on February 7, 2025. As outlined in greater detail below, there remain ongoing issues with the manner in which the government produced the discovery. These complications have impaired the defense's ability to prepare its suppression motions, which are currently due on March 31, 2025. For the reasons expressed herein, defense counsel requires additional time to file full suppression motions.

On January 27, 2025, the defense filed its Motion to Strike Statutory and Non-statutory Aggravators. The government's response was filed on March 14, 2025, and the defense reply is due on April 14, 2025.

On February 3, 2025, the parties filed their Joint Proposed Voir Dire and Jury Selection Procedures. *See* ECF No. 271. The defense simultaneously filed its Memorandum of Law in support of its requested procedures. ECF No. 272.

Additional and substantial litigation and meetings have taken place with respect to the defense Motion for Records Pursuant to JSSA filed on July 21, 2022. ECF No. 10. The government initially responded on August 12, 2022; and the defense replied on August 17, 2022.

Following discussion at the status conference on February 2, 2024, the parties met on March 21, 2024. By letter to the Court on April 26, 2024, the parties outlined their efforts to resolve aspects of the JSSA litigation and requested a meeting with the Jury Administrator (ECF No. 155). On May 17, 2024, the Jury Administrator provided general information relating to whether materials existed, the format of the materials, and whether the materials could be easily redacted (ECF No. 169) and an update to this information was filed on June 18, 2024 (ECF No. 184). On July 12, the defense provided the Court with a status update on this motion July 12, 2024 (ECF No. 187), and its Motion to Preserve JSSA Records (ECF No. 186) on July 15, 2024.

By Text Order entered July 16, 2024, the Court granted that preservation motion, ECF No. 189, and by Decision and Order, July 17, 2024, granted in part, denied in part and deferred in part the request for records related to grand jury selection. ECF No. 190. In accordance with that order, the parties were given access to records from the Jury Administrator under seal on August 7, 2024 (ECF No. 199). Following oral argument on September 13, 2024, the Court issued a Text Order on September 17, 2024, granting the defense access to certain additional records and ordering the Jury Administrator to meet with the parties to answer remaining questions about other requests. ECF No. 214. Access to these additional records was given on September 25, 2024 (ECF No. 217).

Based on its review of the records disclosed up to that point, on October 10, 2024, the defense submitted proposed questions for the Jury Administrator under seal (ECF No. 261), after which the parties met with the Jury Administrator and Chief Deputy Clerk on October 17, 2024. The parties were provided with the Jury Administrator's answers to the October 10, 2024, questionnaire on November 18, 2024 (ECF No. 261-1). In mid-November of 2024, the Court provided responsive data from the Jury Administrator to the parties via email, and the parties

reviewed hard copies of additional Jury Administrator materials on November 18, 2024, at the Buffalo Courthouse. That same day the defense emailed a request regarding missing materials under seal (ECF No. 261-2). Additional review of the materials was conducted on November 19, 2024, and the Court provided the Jury Administrator's response regarding the missing materials that same day. (ECF No. 261-3). On December 20, 2024, the defense made a request for further materials from the Jury Administrator (ECF No. 262). By Decision and Order entered March 12, 2025, the Court granted in part and denied in part the defense access to records. ECF No. 286.

In short, a substantial amount of litigation has taken place since the government filed its NOI just fourteen months ago. The Court has held in person proceedings for oral argument and/or status updates on various aspects of the litigation on nine occasions since the NOI was filed on January 12, 2024. *See* ECF No. 130, 135, 172, 211, 230, 237, 253, 275 and 287).

II. ARGUMENT

As demonstrated at the outset, counsel's request for an adjournment of the trial schedule puts the trial commencement date well within the average pace of capital litigation in the Second Circuit over the last 25 years. The current schedule does not adequately account for counsel's obligations in death penalty cases. Nor does the schedule take into consideration the voluminous discovery generated by the government's investigation and the attendant discovery issues caused by the government's production methods, and the significant remaining litigation required before the commencement of trial.

a. BEGINNING IN PERSON VOIR DIRE ON SEPTEMBER 8, 2025, WOULD REQUIRE AN UNREASONABLY COMPRESSED AND ULTIMATELY INFEASIBLE SCHEDULE FOR THE REMAINING PRETRIAL LITIGATION EVEN ASIDE FROM SUPPRESSION MOTIONS.

Consistent with the significantly shorter time period between indictment, NOI and the beginning of trial in this case as compared to other federal death penalty prosecutions in the Second Circuit, attempting to complete the pretrial litigation that remains to be conducted, even aside from the suppression motions, would result in an unreasonably compressed schedule that would deprive the parties of an adequate opportunity to properly raise and address critically important issues in this matter. Over the next few weeks alone, defense counsel are scheduled to file: a comprehensive motion raising matters relating to the government's presentation of victim impact evidence (March 31, 2025); a motion to change venue (March 31, 2025); a proposed juror questionnaire (April 4, 2025); a reply to the government's response to their Supplemental Memorandum in Support of Motion to Dismiss Counts 11-20 for Failure to State an Offense (April 7, 2025); a reply to the government's 70-page response to their 43-page Motion to Strike Statutory and Non-Statutory Aggravating Factors (April 14, 2025); and a written proffer of evidence to be submitted at an evidentiary hearing on their Motion to Strike the Death Penalty as a Possible Punishment in this Case (May 1, 2025).

The existing scheduling order already contains deadlines for filing pleadings in May, June and August, three of the following four months that remain until the trial is scheduled to start on September 8, 2025. In May, the parties will also be required to review thousands of completed juror summonses. They will also be conducting the multi-day evidentiary hearing on the *Roper* motion, for which the government recently gave notice that it will be presenting the testimony of five different expert witnesses whose direct examinations alone are anticipated to last a total of 24-28 hours. Between approximately July 1 and July 14, 2025,[5] the parties are

[5] These dates are taken from the Joint Proposed Jury Selection Procedures, (ECF No. 271), which to date have not been adopted by the Court.

scheduled to receive up to 1,200 completed juror questionnaires which they must review in time to prepare and exchange their respective lists of proposed stipulated strikes for cause, confer and prepare a final agreed-upon list by August 11, 2025.

Yet to be scheduled are deadlines for filing: grand and petit jury composition challenges; guilt and penalty phase exhibit lists, witness lists, Rule 404(b) and non-mental health expert disclosures; guilt and penalty phase motions in limine, responses and replies, including *Daubert* motions; and guilt and penalty phase proposed jury instructions, proposed verdict forms, memoranda of law in support of any areas of disagreement between the parties, and responses and replies thereto. Even without allowing for oral argument on any of these matters, an attempt to incorporate them into the existing calendar prior to a trial date of September 8, 2025, results in a plainly unworkable schedule:

CALENDAR FOR IN PERSON VOIR DIRE COMMENCING ON SEPTEMBER 8, 2025	
Date	**Filing(s)**
03/26/2025	Gov. Reply, *US v. Rui Jiang* (Motion to Dismiss Count 27)
03/28/2025	Def. Reply, 924(c)
03/31/2025	Def. Motion to Change Venue Def. Challenges to Victim Impact Evidence Def. Motions to Suppress
04/04/2025	Simultaneous Submissions of Proposed Juror Questionnaires Guilt Phase Exhibit Lists, Witness Lists, Expert Disclosures
04/07/2025	Def. Reply Re 924(c) and Supplemental Submission Re *Delligatti*

CALENDAR FOR IN PERSON VOIR DIRE COMMENCING ON SEPTEMBER 8, 2025	
Date	**Filing(s)**
04/14/2025	One step summons/qualification forms mailed to all prospective jurors from Master Jury Wheel. [6] Def. Reply Re: Aggravating Factors.
04/21/2025	Gov. Response Re *Delligatti*
04/28/2025	Def. Reply Re *Delligatti*
05/01/2025	Def. FDPA Proffers
05/02/2025	Guilt Phase Motions in Limine
05/05/2025	One step summons/qualification forms for all prospective jurors from Master Jury Wheel to be returned, distributed to court and parties by this date.
05/12/2025	Parties to Exchange Proposed Guilt Phase Jury Instructions and Verdict Forms
05/09/2025	Gov. Response, Motion for Change of Venue Gov. Response, Motion re Victim Impact Evidence
05/19/2025	Defense 12.2 Notice
05/xx/2025	*Roper* Hearing
05/26/2025	Court to excuse all unqualified/exempt prospective jurors from Master Jury Wheel List by this date.
05/26/25 or 05/19/23	Parties submit proposed instructions for jurors summoned to complete Juror Questionnaires.
05/30/25	Responses, Guilt Phase Motions in Limine

[6] This is an estimated date to ensure compliance with the joint proposed requirement that "the Court, with input from the parties, has three weeks to review and make the determinations of juror qualifications and exemptions." *See* Joint Proposed Voir Dire and Jury Selection Procedures, ECF No. 271 at 1. The standard summons form allows prospective jurors 10 days from receipt of the form in which to return it to the court.

CALENDAR FOR IN PERSON VOIR DIRE COMMENCING ON SEPTEMBER 8, 2025	
Date	**Filing(s)**
06/02/25	Gov. Motion for Rule 12.2 evaluation
06/10/25	Def. Replies, Venue/VIE
06/16/25	Def. Response to gov Motion for 12.2 evaluation Replies, Guilt Phase Motions in Limine Penalty Phase Exhibit Lists, Witness Lists, Non-Mental Health Expert Disclosures Joint Proposed Guilt Phase Jury Instructions and Verdict Forms and Memoranda in Support of Areas of Disagreement Parties to Exchange Proposed Penalty Phase Jury Instructions and Verdict Forms
06/23/25	Gov. Reply, Motion for 12.2 evaluation
06/23/25 or 06/16/23	Panels to court to complete Juror Questionnaires begins
06/30/25	Completion of Juror Questionnaires by all panels by this date
07/14/25	All completed Juror Questionnaires provided to parties in pdf format by this date Penalty Phase Motions in Limine Responses, Guilt Phase Jury Instructions and Verdict Forms Memoranda in Support of Areas of Disagreement Joint Proposed Penalty Phase Jury Instructions and Proposed Verdict Forms Memoranda in Support re Areas of Disagreement
07/28/25	Replies, Guilt Phase Jury Instructions and Verdict Forms Memoranda in Support of Areas of Disagreement
08/11/25	Parties submit to Court list of stipulated strikes for cause and hardship Responses, Penalty Phase Motions in Limine Responses, Memoranda in Support of Proposed Penalty Phase Jury Instructions and Proposed Verdict Forms

CALENDAR FOR IN PERSON VOIR DIRE COMMENCING ON SEPTEMBER 8, 2025	
Date	**Filing(s)**
08/25/25	Replies, Penalty Phase Motions in Limine Replies, Memoranda in Support of Proposed Penalty Phase Jury Instructions and Proposed Verdict Forms
09/08/25	Start of In Person Voir Dire

This schedule would also have to somehow include the filing of defense motions to suppress, responses thereto, replies and any necessary oral arguments and evidentiary hearings, as detailed below

b. THERE ARE COMPLEX FOURTH AMENDMENT ISSUES IN THIS CASE ARISING FROM THE GOVERNMENT'S SEARCH AND SEIZURE OF VAST QUANTITIES OF DIGITAL DATA FROM PAYTON GENDRON'S ELECTRONIC DEVICES AND ONLINE ACCOUNTS THAT CANNOT BE PROPERLY RAISED AND ADJUDICATED IN THE TIME AVAILABLE BEFORE THE CURRENTLY SCHEDULED TRIAL DATE.

While the same is certainly not true in all cases, the suppression issues in this case are abundant, meritorious and both legally and factually complex. This is so primarily because of the vast amount of digital evidence searched and seized by the government and the Fourth Amendment issues that are implicated as a result. However, because of multiple, still unresolved problems with the way in which discovery has been produced to the defense team, we have yet to be able to complete and file the necessary motions to suppress and there is insufficient time before the currently scheduled trial date to adequately litigate and resolve them.

The digital age has necessitated and continues to necessitate judicial reassessment of large swathes of Fourth Amendment doctrine in an effort to ensure that constitutional protections keep pace and adapt in a world of rapidly changing technologies that have completely

revolutionized the ways that most of us live our lives. *See Carpenter v. United States*, 585 U.S. 296, 305 (2018) ("As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted'") (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)); *United States v. Ganias*, 824 F.3d 199, 209 (2d Cir. 2016) (en banc) (explaining that, although no conclusion reached regarding existence of Fourth Amendment violation due to decision on other grounds, "we make some observations . . . both to illustrate the complexity of the questions in this significant Fourth Amendment context and to highlight the importance of careful consideration of the technological contours of digital search and seizure for future cases"). Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrate's Revolt*, 68 Emory L. J. 49, 51 (2018) ("The information age has created an avalanche of Fourth Amendment-law dilemmas . . . It is up to courts in the first instance to resolve these questions").

In 2014, the Supreme Court held that, as a general matter, law enforcement officers must obtain a search warrant in order to search the digital contents of a cellphone, even when the device itself is seized incident to arrest. *See Riley v. California*, 573 U.S. 373, 386, 401 (2014). In so doing, the Court recognized that even the term itself is "misleading," for "many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Id.* at 393. To which filing cabinets, safe deposit boxes, storage lockers, credit cards, credit card and bank statements, love letters, medical files, trackers of sleep, exercise and vital signs, and a complete record of where the

owner is located at every moment may be added, to name just a few additional functions of a smart phone in this day and age.

More recently, it has become common to store this type of comprehensive, highly personal and private information not on the cellphone itself, but in the "cloud," a virtually unlimited storage space that can be accessed using the device by the click of a few buttons. Third-party companies and entities that operate in the cloud gather and store enormous amounts of our information, such as email accounts and associated contacts lists, instant messages, social media accounts, internet browsing history, access points known as IP addresses and much, much more. In recognition of this phenomenon, in 2018 the Supreme Court held that, notwithstanding the fact that such data is in the possession of a third-party, the user may nevertheless maintain a reasonable expectation of privacy in their own content such that a warrant based on probable cause is required before law enforcement may demand access. *Carpenter*, 585 U.S. at 310, 311, 316 (holding that warrant is required for individual's cellphone location information and noting that such information "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations . . . [in short,] for many Americans the privacies of life") (internal quotations omitted).

While groundbreaking, the decision of the Supreme Court in *Carpenter* left open at least as many thorny questions about the scope of Fourth Amendment protection in this area as it answered. With respect to digital devices, such as computers, laptops and cellphones, courts generally agree that individuals have a privacy interest protected by the Fourth Amendment. *See, e.g., United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) ("Generally, people have a reasonable expectation of privacy in the contents of their home computers.") Privacy

concerns may be even more significant when it comes to digital and online accounts, such as those used for email, text messaging, internet searching and social media. *See United States v. Shipp*, 392 F. Supp. 3d 300, 307-08 (E.D.N.Y. 2019) (noting that "threat [to privacy] is further elevated in a search of Facebook data because, perhaps more than any other location—including a residence, a computer hard drive, or a car—Facebook provides a single window through which almost every detail of a person's life is visible").

The issues are more complex and fact-intensive, however, with online accounts: "Facebook—and social media generally—present novel questions regarding their users' expectations of privacy." *Id.* As the district court explained in *Meregildo*:

> Facebook users may decide to keep their profiles completely private, share them only with 'friends' or more expansively with 'friends of friends,' or disseminate them to the public at large . . . Whether the Fourth Amendment precludes the Government from viewing a Facebook user's profile absent a showing of probable cause depends, *inter alia*, on the user's privacy settings.
>
> When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. However, postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected.

Id.

Courts have employed a two-prong approach to determining whether a defendant has a constitutionally protected privacy interest in the contents of his social media accounts. "First, when evaluating whether a defendant manifested a subjective expectation of privacy, courts consider whether the defendant intentionally took steps to avoid 'allow[ing] the public at large to access' pertinent evidence." *United States v. Chavez*, 423 F. Supp. 3d 194, 201-02 (W.D.N.C. 2019) (quoting *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010)). "Second, this Court must determine whether defendant's subjective expectation of privacy is reasonable." *Id.* at 202.

The *Chavez* court concluded that, indeed, "it is objectively reasonable for an individual to expect privacy in non-public content that is entrusted to a social media website as the intermediary of the ultimate recipient . . . To read the Constitution as entirely failing to protect such private information 'is to ignore the vital role that [social media] has come to play in private communication.'" *Id.* at 203-204 (quoting *Katz v. United States*, 389 U.S. 347, 352 (1967)). Accordingly, the court found that the defendant had a reasonable expectation of privacy in the non-public content of his Facebook account, notwithstanding the fact that he had chosen to share it with the 300-400 individuals he had accepted as "friends" on the site. *Id.* 200, 204-05. *See also United States v. Zalaya-Veliz*, 94 F.4th 321, 333 (4th Cir. 2024) (noting that "[m]ost federal courts to rule on the issue have agreed that Facebook and other social media users have a reasonable expectation of privacy in content they exclude from public access, such as private messages"); *In re Three Hotmail Email Accounts*, No. 16-MJ-8036-DJW, 2016 WL 1239916, *13 (D. Kan. Mar. 28, 2016) (objections sustained in part on other grounds by *In re Search of Info. Assoc. With Email Addresses Controlled by Microsoft Corp.*, 212 F. Supp. 3d 1023 (D. Kan. 2016)) (holding that answer to question of whether an individual has right to privacy in his email account is "unequivocally yes;" further explaining that "privacy concerns not only our interest in determining *whether* personal information is revealed to another person but also our interest in determining *to whom* such information is revealed"); Kenneth L. Karst, *The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data,* 31 L. & Contemp. Probs. 342, 346 (1966) ("Meaningful discussion of privacy requires the recognition that ordinarily we deal not with an interest in total nondisclosure but with an interest in selective disclosure").

For searches of electronic devices and, where applicable, social media and other online accounts, law enforcement must obtain a valid search warrant that is based on probable cause to

believe not only that a crime has been committed, but also that evidence of that crime will be found on the device or digital account that law enforcement wishes to search. *See United States v. Parker*, No. 22-CR-6203, 2023 WL 6156268, at *2 (W.D.N.Y. Sept. 21, 2023) ("'To establish probable cause . . . two factual showings are necessary—first, that a crime was committed, and second, that there is probable cause to believe that evidence of such crime is located [on the device/account]'") (quoting *United States v. Travisano*, 724 F.2d 341, 345 (2d Cir. 1983)). "'[P]robable cause to search [a device] exists of the issuing judge finds a fair probability that . . . evidence of a crime will be found' therein. *Id.* (quoting *United States v. Ponce*, 947 F.2d 646, 650 (2d Cir. 1991)).

In other words, a "nexus" must be shown between the device and the alleged criminality. *Id.*; *see also Chavez*, 423 F. Supp.3d at 206 (noting requirement that government establish probable cause to believe that relevant evidence may be found in defendant's Facebook account); *United States v. Ulbricht*, 858 F.3d 71, 104 (2d Cir. 2017) (finding "ample basis" to conclude that evidence of crime "likely permeated Ulbricht's computer . . . given the nature of Ulbricht's crimes and their symbiotic connection to his digital devices"); Jennifer S. Grannick, *Making Warrants Great Again: Avoiding General Searches in the Execution of Warrants for Electronic Data*, 47 Champion 28, 29 n.20 (2023) (noting that appendix to ACLU's whitepaper, Making Warrants Great Again, contains amicus briefs challenging search warrants on grounds of lack of nexus); ACLU, *The Warrant Clause in the Digital Age* (May 3, 2023) https://www.aclu.org/cases/digital-age-warrants (last visited March 17, 2025).

A search warrant must also define the scope of the search it authorizes with particularity. "The particularity requirement has three components. First, a warrant must identify the specific offense for which the police have established probable cause. Second, [it] must describe the

place to be searched. Third, the warrant must specify the items to be seized by their relation to designated crimes." *United States v. Galpin*, 720 F.3d 436, 445-46 (2d Cir. 2013) (internal quotations and citations omitted). "'[A]n otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based.'" *Id.* at 446 (quoting 2 W. LaFave, *Search and Seizure* § 4.6(a) (5th ed. 2012)). With "as much particularity as the circumstances reasonably allow," nothing about what may and may not be seized is to be left to the discretion of the officer executing the warrant. *Id.*

Due to the amount of potentially accessible data and its often highly sensitive nature, when "the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance." *Id.*; *see also Three Hotmail Email Accounts*, 2016 WL 1239916, at *10 n. 70 (same); *Galpin,* 720 F.3d at 450 (finding invalid portion of warrant to search computer that, while particularizing the items to be seized, offered no explanation of "how the vast majority of those items—*e.g.*, access numbers, passwords, and PINS relating to voice mail systems, computing or data processing literature (including written materials), audio or video cassette tape recordings, books, and magazines—could possibly reveal evidence" of crime at issue).

The same is true when law enforcement seeks access to a social media or other online account. *See, e.g., Chavez*, 423 F. Supp. 3d at 206-07 (finding warrant for defendant's Facebook account requiring disclosure of "'virtually every type of data that could be located in a Facebook account'" so overbroad that it violated particularity requirement of Fourth Amendment) (quoting *United States v. Blake*, 868 F.3d 960, 966 (11th Cir. 2017)); *Three Hotmail Email Accounts*, 2016 WL 1239916, at *13 ("The Court remains concerned that each of the target email accounts

may—and likely do—contain large numbers of emails and filed unrelated to the alleged crimes being investigated and/or for which the government has no probable cause to search or seize.") .

From a practical perspective, when law enforcement agencies seek access to digital information stored on a cellphone, laptop or desktop computer, tablet or other device, they often utilize a two-step process: first, capturing all of the data stored thereon, and second, thereafter searching the captured data and seizing that which is relevant, i.e., authorized by the warrant and supported by probable cause. As Judge Chin of the Second Circuit has explained:

> In the computer age, off-site review has become much more common. The ability of computers to store massive volumes of information presents logistical problems in the execution of search warrants, and files on a computer hard drive are often 'so intermingled that they cannot feasibly be sorted on site.' Forensic analysis of electronic data may take weeks or months to complete, and it would be impractical for agents to occupy an individual's home or office, or retain an individual's computer, for such extended periods of time. It is now also unnecessary. Today, advancements in technology enable the government to create a mirror image of an individual's hard drive, which can be searched as if it were the actual hard drive but without otherwise interfering with the individual's use of his home, office, computer, or files.

Ganias, 824 F.3d at 230-31 (Chin, J., concurring) (quoting *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982)). *See also Three Hotmail Email Accounts*, 2016 WL 1239916, at *2-3, (noting that '[l]aw enforcement commonly images a seized hard drive in order to perform a search of the data at their forensic lab"); Berman, *supra*, at 57 ("the nature of digital evidence requires investigators to seize entire storage devices and search them for evidence later . . . rather than seizing only evidence of criminality from the outset"). The Federal Criminal Procedure Rules explicitly countenance this procedure. *See* Fed. R. Crim. P. 41(e)(2)(B) (*Warrant Seeking Electronically Stored Information*) ("A warrant . . . may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant").

However, executing a digital search in this manner means that law enforcement officers routinely gain to access large amounts of data for which they unquestionably lack probable cause. *See* Berman*, supra,* at 58 ("'over-seizing is an inherent part' of digital evidence collection") (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (2020)*; Ganias*, 824 F.3d at 230-31 (Chin, J., concurring) ("for these practical considerations, the Government may, consistent with the Fourth Amendment, overseize electronically stored data when executing a warrant. But overseizure is exactly what it sounds like. It is a seizure that *exceeds* or *goes beyond* what is otherwise authorized by the Fourth Amendment"); *Ulbricht*, 858 F.3d at 99 ("Because of the nature of digital storage, it is not always feasible to extract and segregate responsive data from non-responsive data, creating a serious risk that every warrant for electronic information will become, in effect, a general warrant") (internal quotations omitted).

This two-step search and seizure process therefore requires a two-step analysis for Fourth Amendment purposes. Courts must first determine whether the search warrant validly authorizes the initial seizure of the device and the data contained therein. Then, the reasonableness of the subsequent review and extraction of "relevant" content must be assessed. *See Ganias*, 824 F.3d at 231-32 (Chin, J., concurring) ("To safeguard individuals' possessory and privacy interests, when the government seeks to review mirror images off-site, we are careful to subject the Government's conduct to the rule of reasonableness."); Grannick, *supra*, at 30 ("Yet, *seize first, search second*, is not always constitutional. Any overseizure must still be 'reasonable' within the meaning of the Fourth Amendment. Rule 41 does not (and constitutionally could not) authorize seizures of data that are unnecessary or unreasonable in the context of a particular investigation"). "The first step to protecting Fourth Amendment interests is to limit the amount

of nonresponsive data that may be accessed by law enforcement in the first instance. The second step is for the warrant to limit searches of that data." *Id.* at 33.

A storage device such as a cellphone or laptop might not organize raw data by category or in other easily discernable ways, necessitating initial production of the device's entire contents. However, readily available digital forensic tools for extracting and searching that data typically do sort the information into categories, and review can and should thereafter be limited to those which are relevant and for which probable cause has been established:

> Information in a cell phone cannot be examined comprehensively while it is in the phone. Technicians employ software— here, from the Cellebrite company—to conduct forensic examinations of cell phones in two stages. In the first step, all or nearly all the electronic data in the device is copied into another computer and organized for examination—in effect, the information is dumped on a table so it can be reviewed. *See United States v. Palms*, 423 F. Supp. 3d 1254, 1258 (N.D. Okla. 2019). It is as if the warrant had authorized the search of a trove of documents written in Mandarin. The documents would have to be translated into English before being read by officials knowledgeable about the case. In short, this information "dump" yields readable reports of electronic information, segregated by type into files which an examiner can open.
>
> . . .
>
> In the second step, an examiner with knowledge of the case and of the warrant authorization sifts through the information in the files to locate relevant material. *United States v. Palms*, 423 F. Supp. 3d at 1258-59, *supra; see also United States v. Graziano*, 558 F. Supp. 2d 304, 313-14 (E.D.N.Y. 2008). It is this second step that is the actual search for the evidence sought by the authorities—the "key issue for both the issue of particularity and the scope of the search is the actual review of the Cellebrite reports." *United States v. Palms*, 423 F. Supp. 3d at 1263-64, *supra*. A search is therefore consistent with the Fourth Amendment if the warrant properly limits the examination of the "dumped" information at the second step.

People v. Musha, 131 N.Y.S. 3d 514, 517-18 (Sup. Ct. 2020). In *Musha*, police obtained a warrant to search a cell phone belonging to a defendant charged with child sexual abuse. *Id.* at 516. The court found that the warrant validly authorized the seizure of certain photographs and two days' worth of call logs from the device, but that it failed to establish probable cause to comb through the defendant's internet search history for evidence of a sexual interest in young girls. *Id.*

at 522-23. It therefore suppressed that evidence. *Id.* at 523. Similarly, a warrant that authorized unlimited access to all types of data on a defendant's cell phone was found invalid in *People v. Thompson*, 116 N.Y.S. 3d 2, 3-4 (App. Div. 2019), where probable cause existed only for a search of a single day's call logs and text messages.

With respect to online accounts such as social media, no similar justification for a "demand disclosure of everything first, search and seize later" approach by law enforcement exists. When the companies that maintain these accounts produce their contents in response to a search warrant, the data is already organized by category; disclosure can therefore be limited in the same way. *See, e.g., Shipp*, 392 F. Supp. 3d at 304-05 (listing 16 categories of Facebook data required to be disclosed by search warrant); *Chavez*, 423 F. Supp. 3d at 199 (same). In some instances, disclosure can be limited to less than an entire category. *See* Grannick, *supra*, at 31-32 (noting that data from Google Gmail accounts can be restricted by date, sender and recipient, and Google Photos is organized in such a way that demands can be limited to only images taken at a particular location or containing the face of a particular person). Thus, "[w]hatever the merits of a *seize first, search second* approach in the context of computer hard drives the same considerations do not justify seizures of data in an email or social media account." Grannick, *supra*, at 30.

At a minimum, then, a search warrant for such an account must limit the categories of data that may be searched and seized to those that are relevant, i.e., supported by probable cause. If a warrant for a digital account fails to appropriately limit the required disclosure, it violates the Fourth Amendment. *See Chavez*, 423 F. Supp. 3d at 206-07 (finding warrant for defendant's Facebook account requiring disclosure of "'virtually every type of data that could be located in a

Facebook account'" so overbroad that it violated particularity requirement of Fourth Amendment) (quoting *United States v. Blake*, 868 F.3d 960, 966 (11th Cir. 2017)).

Another important consideration when assessing the validity of a search warrant, whether for a device or an account, is whether it contains an appropriate temporal limitation. An authorized search should be no broader than the date range for which probable cause to believe that evidence of the crime may be located has been established. *See Shipp,* 392 F. Supp. 3d at 310 ("'A warrant's failure to include a time limitation, where such limiting information is available and the warrant is otherwise wide-ranging, may render it insufficiently particular.'") (quoting *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 464 (S.D.N.Y. 2013); *Chavez*, 423 F. Supp. 3d at 207 (finding warrant overbroad where it compelled Facebook to disclose 16 broad categories of information without limiting to dates on which crime was believed to have been committed); *Zelaya-Veliz*, 94 F.4th at 339 ("'By narrowing a search to the data created or uploaded during a relevant time connected to the crime being investigated, officers can particularize their searches to avoid general rummaging.'") (quoting *United States v. McCall*, 84 F.4th 1317, 1328 (11th Cir. 2023)); *In re Search of Google Email Accounts Identified in Attachment A*, 92 F. Supp. 3d 944 (D. Alaska 2015) (denying as overbroad application for warrant to search entirety of email accounts without date restriction).

In addition to limiting the amount of data required to be disclosed, the Fourth Amendment may also require law enforcement to utilize search protocols and techniques to minimize the intrusion into privacy interests when reviewing that data. "Were courts to adopt the argument that police can look at all the information they seize, there would be no meaningful limit to searches or seizures of digital information." Grannick, *supra*, at 33. *See also* Berman, *supra*, at 83 ("The challenge [with digital searches] is to devise a way to limit post-collection

privacy intrusions"). Courts have taken a variety of approaches to implement this principle, including enforcing time limits within which the search process must be completed, *see United States v. Mutschelknaus*, 592 F.3d 826, 829-30 (8th Cir. 2010) (affirming denial of motion to suppress computer data seized pursuant to warrant requiring search within 60 days of recovery of device); *United States v. Brunette*, 76 F. Supp. 2d 30, 42 (D. Me. 1999) (suppressing evidence sized from computer where law enforcement failed to complete search with 30 days as specified in warrant); limiting who may have access to the data in this first instance, *Three Hotmail Email Accounts*, 2016 WL 1239916, at *18-19 (noting government has option to set up filter team of trained computer personnel separate from investigators and operating behind a firewall to review information); imposing restrictions upon access to and use of data after review has been completed, *id.* at *23 ("The government should not be permitted to indefinitely seize non-responsive data, especially if it is permitted to overseize [] in the first place;" courts may require that it be returned or destroyed after search completed); and directing the use of search protocols such as keyword searches or restrictions to certain file types, *id.* at *19-20 (noting that lack of particularity may in some circumstances be cured by the government's use of a search protocol limiting its access to overseized data).

Resolution of many of these questions requires extensive factual investigation and determination; evidentiary hearings are therefore frequently required. *See, e.g., Galpin*, 720 F.3d at 443-44 (noting that district court held evidentiary hearing on suppression motion including testimony of government's computer forensics analyst about her search methods, use of word searches, segregation of different file types for opening and individual examination, how she decided what to search and seize and what not to, and information about investigation she was provided with beforehand, and emphasizing need for court to "develop a record as to the proper

scope and conduct of a search for evidence" to inform questions remaining for resolution on remand); *Ganias*, 824 F.3d at 207-08 (noting that district court conducted two-day hearing on motion to suppress evidence seized after forensic examination of mirrored computer hard drives pursuant to warrants); *Chavez*, 423 F. Supp. 3d at 200 (noting that hearing was conducted on motion to suppress data from defendant's Facebook account that included introduction of evidence of privacy restrictions available to users and chosen by defendant and search procedures performed by law enforcement).

In this case, in addition to two warrants for the search of Payton Gendron's car and two for the search of his home, law enforcement obtained 15 warrants for digital data from 12 different devices and nine separate online accounts. For each of the 15 warrants, to determine whether a motion to suppress is appropriate, the defense team must identify and review in the more than four terabytes of discovery materials: the search warrant, the affidavit in support thereof and the return; the data set that was produced by the company in response to the warrant; all documents that pertain to the process utilized by law enforcement to search that data set; and the subsets of data that the reviewing officers deemed "relevant" and seized during the search process. With respect to both the initial data set and the seized portions, we must assess: whether the search warrant was supported by probable cause to believe a crime had been committed and that evidence thereof was reasonably likely to be found on the device or in the account searched; whether the warrant sufficiently particularized the categories of data that could be searched and those which could be seized; whether it properly limited each category to data for which probable cause existed; whether the search protocols employed sufficiently minimized the intrusions upon privacy for which no probable cause existed; whether the seized data was in fact

within the scope of the seizure authorized by the warrant; and whether the remaining data was appropriately disposed of when the search process was complete.

In addition, before seeking any of these warrants law enforcement made at least nine separate requests for Voluntary Emergency Disclosure ("EDR's") of Payton Gendron's digital data directly to the companies that operate and store that data pursuant to the Stored Data Communications Act, 18 U.S.C. §§ 2701 *et seq*. Pursuant to that statute, an internet service provider is permitted to disclose an individual's confidential subscriber data to law enforcement if it "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." 18 U.S.C. § 2702(c)(4).

In this case, three of the companies to which EDR's were submitted denied the request on the ground that the requesting officers had failed to establish the existence of an emergency within the meaning of the statute. Others did disclose data, separately violating Payton Gendron's Fourth Amendment rights. Furthermore, data that was illegally obtained in this manner was subsequently relied upon to establish probable cause for search warrants, raising complex issues under the fruit of the poisonous tree doctrine.

To date, the defense team has been prevented from completing the process of preparing motions to suppress by their inability to reliably identify the subsets of data that the reviewing officers deemed "relevant" and seized during the search process in each instance, as well as the data initially disclosed in some instances. The FBI stores this data as "attachments" to its form reports. However, as we have previously explained to the Court, (ECF Nos. 246-47), because of how discovery was initially produced to us we were unable to determine which "attachments"

were associated with which reports and thus, as relevant here, which subsets of data were disclosed and/or seized in connection with which search warrant or EDR.

We identified this problem as we began to research and prepare to file suppression motions in the Spring and Summer of 2024 and, in July of 2024, we requested in writing to the government that it provide us with a mechanism to remedy the issue. Despite agreeing to provide us with the requested information, however, and informing us on multiple occasions over the ensuing months that it was in the process of complying with our request, we received no additional information from the government until October 24, 2024. And on that date, as the Court is aware, we were presented with a reissued set of discovery with brand new Bates numbers, together with a spreadsheet or manifest that almost completely failed to accomplish the purpose for which it was supposedly created. (ECF Nos. 246-47.)

At a status conference held on December 11, 2024, the Court ordered the government to "identify by original Bates number all attachments associated with each report and to provide the original Bates number for all documents it reproduced with a new Bates number" by January 13, 2025. (ECF No. 253.) The government applied for and was granted two extensions of time to comply with the Court's Order, (ECF Nos. 259, 263), and a status conference to review the status of its compliance was rescheduled from January 30, 2025, to February 7, 2025, (ECF No. 264). Finally, at 10:00pm on the night of February 6, 2025, the government sent defense counsel by email a revised copy of its manifest in purported compliance with the Court's December 11, 2024, Text Order. In a cover letter, the government represented that "[i]n creating the second revised discovery manifest, the FBI completed an exhaustive audit of its file to ensure that the manifest identified each and every report that has been disclosed and the corresponding attachments for each report."

Following the status conference on February 7, 2025, the defense team ingested the government's Second Revised Manifest into the database program that houses our discovery index, linked the manifest with our index in order to begin to marry up our years' worth of existing work product with the new information, and began to evaluate whether the attachments and other issues were sufficiently resolved to permit the identification and isolation of the data sets relevant to potential suppression motions. We immediately ran into continuing problems, including: (1) entries for 1B physical attachments that did not pertain to their respective reports; and (2) nothing in the manifest that directed us to where the 1B physical attachments could be found.[7] We brought these issues to the government's attention in a February 19, 2025, letter.

On February 25, 2025, we met with the government to address these issues. Twenty minutes before the meeting began, the government sent yet another revised version of the manifest, which we reviewed to the extent possible during the meeting.[8] The government represented that it had fixed the incorrect 1B attachments and added UID numbers and hard-

[7] We also found continuing issues with the governments Bates- numbering and re-numbering, including: (1) entries in the Prior Bates column that were above GOV-00080975, which meant they must be new rather than prior Bates numbers; and (2) entries marked N/A, indicating no prior Bates number existed, when spot checks revealed that the reports had in fact been numbered and produced in prior discovery.

[8] This version addressed the issue of numbers placed in the Prior Bates column that were in fact new Bates numbers. During the meeting the government represented that we had incorrectly marked N/A entries for Prior Bates and that it had reviewed and verified the correctness of all such entries; however, we continue to find Prior Bates marked N/A where, with significant expenditure of time and effort, we can identify prior discovery documents that indeed appear to have been duplicated with new Bates numbers. We have also found entries that have incorrect Prior Bates numbers that were assigned to entirely different documents, where the Prior Bates numbers refer to reports that are similar but have different FBI Serial numbers, or relate to a single file where the attachment consists of multiple files. The Bates numbering issues noted here are likely unexhaustive, even within the search warrant-related entries upon which our review has focused so far.

drive location information to those entries so they could be located. However, even during the meeting, it became clear that not all of the issues had been fixed, so the government said it would clean these up and send another manifest soon.

On February 26, we received the fifth version of the government's discovery manifest, entitled Third_Revised_Discovery_Manifest_2025-26-02.xlsx ("Third Revised Manifest"). We again ingested this manifest into our database program, re-linked it with our discovery index,[9] and began again to evaluate the attachments issues. Because of the need to complete the preparation of suppression motions, we have concentrated our review initially on search-warrant-related reports and attachments (267 reports and 1,303 total entries). In order to generate a list of reports and attachments related to the warrants, we first had to review each entry in the manifest and fill out the SEARCH WARRANT column. This column already existed in the version provided by the government, but it was only partially filled out, and the entries that were completed were riddled with errors.

We then moved on to assessing the accuracy and completeness of the attachments information for the search warrant-related reports, and found that serious issues still remain uncorrected. There are 1B physical attachment entries that do not have a UID number and hard-drive location, which the government represented is how we can now locate these entries. And, there continue to be attachments mentioned in reports that are not listed in the manifest or otherwise identifiable in the mountain of produced or reproduced discovery. In sum, after a combined total of 66 hours of work, we have determined that, for 40 of 178 reports we have

[9] Every time the government sends us a corrected manifest, we must delete the previous manifest from our database program, upload the new version, and redo the linking process. Any additional work we have done on the manifest is lost and must be redone.

identified as pertaining to the various search warrants, the attachments remain either partially or completely unidentified. We are preparing a written request to the government to supply us with the missing information, and as soon as they comply with this request we can complete preparation of our suppression motions.

c. DEFENSE COUNSEL REQUIRE ADDITIONAL TIME TO COMPLETE THE CONSTITUTIONALLY MANDATED INVESTIGATION REQUIRED TO ADEQUATELY PREPARE FOR THE PENALTY PHASE

Despite our sustained and diligent efforts, the defense team is unable to complete the constitutionally required investigation into Payton Gendron's psychosocial history and comprehensive evaluation of his mental condition within the time remaining until the currently scheduled trial date. Although we have accomplished an enormous amount of work on multiple fronts, and have developed a roadmap for what remains to be done in order for us to be ready to present Payton Gendron's case in mitigation and meet the government's case in aggravation at trial, we need more time in which to finish what is, to put it mildly, a massive undertaking. *See* Ex Parte Supplement in Support of Motion to Adjourn the Trial Date and for a Further Pretrial Scheduling Order filed simultaneously herewith under seal.

III. CONCLUSION

When the Court originally set the current trial date, it did so at the behest of the government and over defense objection. The defense urged the Court to delay the setting of a firm date until such time as a more realistic date for the trial could be set. ECF No. 154. While a trial date of September 8, 2025, was set, this Court cautioned:

> I do think that it makes sense to – and I'm making it clear so, you know, whatever, you know, the media gets this transcript or whoever's here in the courtroom right now is a realistic trial date. *That can change and may change*

> *over the course of the motion practice and discovery that we are engaging in.* But right now, this is what seems to be a realistic time to try the case.
>
> Does that mean it's not going to change the way I say in most cases it's not going to change? No. But it means that it's giving us all something to work toward and something to set our respective schedules with, you know, factoring in. So that's what we're going to do.
>
> And that does not mean that that's a come-hell-or-high-water trial date, but it is the date that is the aspirational trial date, the date we're all going to work toward, the date that gives us something to, as Mr. Tripi says, you know, I was a lawyer for 30 years and I've seen lawyers now for the last eight from this perspective, and I know that unless there are deadlines, sometimes things don't get done. So we're going to set a deadline.

ECF No. 154 at 49-50. The parties have diligently worked toward meeting that aspirational trial date, but as has been demonstrated herein, that date no longer represents a realistic trial date given the legal issues remaining to litigate, the volume of trial related litigation and counsel's need for additional time to complete their mitigation investigation. The requested extension is not unreasonable in light of the average time from charge to trial that similar capital cases have required in this Circuit.

Accordingly, defense counsel asks this Court to continue the present trial date, and set a new trial date and a full pretrial scheduling order as proposed by defense counsel in Exhibit B.

Dated: March 25, 2025
Buffalo, New York

s/Sonya A. Zoghlin
Sonya A. Zoghlin
Assistant Federal Public Defender

s/MaryBeth Covert
MaryBeth Covert
Senior Litigator

s/Julie Brain
Julie Brain
Julie Brain, Attorney at Law

s/Monica Foster
Monica Foster
Executive Director
Indiana Federal Community Defenders Inc.